DC3 Digital Forensics Challenge

203 – Registry Analysis

Team Information

Team Name: Barely Legal

Results Email: [redacted]

Examination Time Frame: to 10/31/08

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided registry files and USB Image files located in the **203_Registry_Analysis_Challenge2008** folder, which of the USB devices was attached to the suspect hard disk drive. Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason for your selections.

Points will be awarded for successfully identified USB device connected to the suspect hard disk drive, provided you supply a detailed methodology of how you determined your findings.

Total Weighted Points: 40 Total Points available per entry – Total 200 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:

Points Awarded:

Date:

Review Period: to

Completed: □ Yes □ No □ Partial

REPORT OF EXAMINATION

203 Registry Analysis

The following USB Device information was recovered from the SYSTEM registry file:

(see next page. The rest of this page is intentionally left blank)

USB Devices List

Created by using USBDeview

Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug Date	VendorID	ProductID
DELL USB Keyboard	USB Human Interface Device	HID (Human Interface Device)	No	Yes	No	No			4/1/2008 3:28:18 AM	N/A	413c	2005
Dell USB Mouse	USB Human Interface Device	HID (Human Interface Device)	No	Yes	No	No			4/1/2008 3:28:18 AM	N/A	413c	3200
Drive AU_USB20	Flash Drive AU_USB20 USB Device	Mass Storage	No	No	No	No		BQENV5CR	3/12/2008 8:11:18 AM	N/A	058f	6387
Flash Disk	USB 2.0 Flash Disk USB Device	Mass Storage	No	No	No	No		A127000000000063	2/14/2008 10:26:30 AM	N/A	090c	1000
LaCie Hard Drive USB	SAMSUNG HD501LJ USB Device	Mass Storage	No	No	No	No		152D203380B6	2/28/2008 2:16:52 PM	N/A	059f	0951
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No	G:	0778102104F1	4/4/2008 8:18:03 AM	N/A	12f7	1d00
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No	I:	0778102B028C	4/1/2008 3:28:18 AM	N/A	12f7	1d00
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No		0778102B05EC	3/21/2008 10:16:45 AM	N/A	12f7	1d00
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No	H:	0778102C0211	4/4/2008 8:18:08 AM	N/A	12f7	1d00
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No	K:	0778102C0441	4/1/2008 3:28:18 AM	N/A	12f7	1d00
TD Classic 003B	Memorex TD Classic 003B USB Device	Mass Storage	No	No	No	No	J:	0778102D041B	4/1/2008 3:28:18 AM	N/A	12f7	1d00

METHODOLOGY / NOTES FORM

203 – Registry Analysis

Date / Time	Notes
31-Oct-08 5:30 pm	Tool(s) Used: EnCase 6.11.2 by Guidance Software (www.encase.com) USBDeview by NirSoft (http://www.nirsoft.net/utils/usbdeview.zip) Created new case in EnCase. Mounted USB images by “Adding Raw Image” in Encase Look for entries in the HKEY_Local_Machine\System\CurrentControlSet\Enum\USBSTOR Acquired Serial numbers of USB devices by using USBDeview on the SYSTEM registry file: `USBDeview.exe /regfile " D:\203_Registry_Analysis_Challenge2008\ Registry Files\SYSTEM"` Found entries that match the volume Serial number of the USB images Volume Serial numbers -------------- USB1: f4d8-dd43 USB2: fd66-9053 USB3: 7c6c-0ed5